APLIKASI PENGAJUAN SURAT MENGGUNAKAN *DIGITAL SIGNATURE* ALGORITMA RSA PADA LPPM UIN SUSKA

TUGAS AKHIR

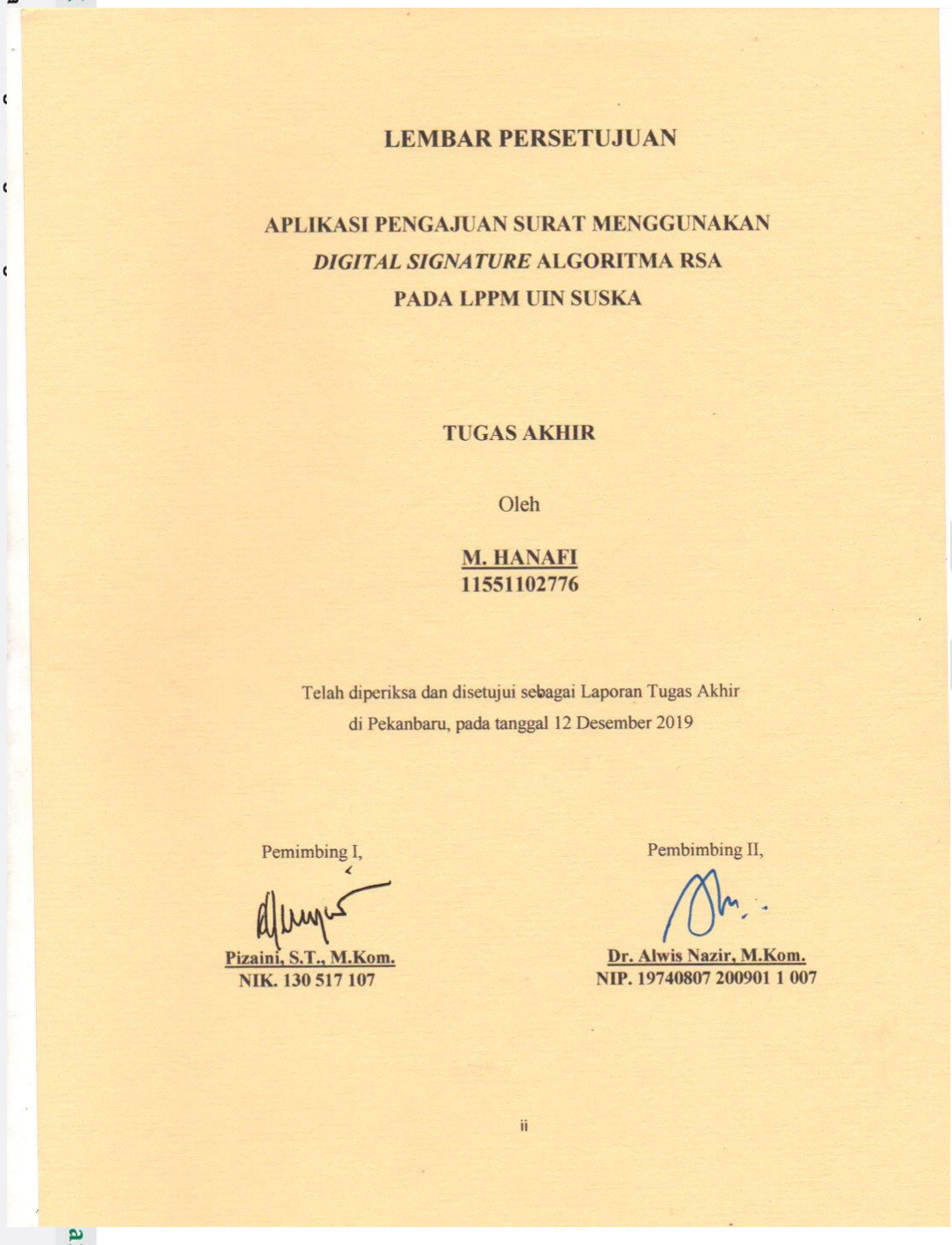
Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik
Pada Jurusan Teknik Informatika

Oleh :

M. HANAFI
11551102776

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
2019

LEMBAR PERSETUJUAN



LEMBAR PERSETUJUAN

APLIKASI PENGAJUAN SURAT MENGGUNAKAN *DIGITAL SIGNATURE* ALGORITMA RSA PADA LPPM UIN SUSKA

TUGAS AKHIR

Oleh

M. HANAFI
11551102776

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 12 Desember 2019

Pemimbing I,

Pizaini, S.T., M.Kom.
NIK. 130 517 107

Pembimbing II,

Dr. Alwis Nazir, M.Kom.
NIP. 19740807 200901 1 007

ii

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

APLIKASI PENGAJUAN SURAT MENGGUNAKAN *DIGITAL SIGNATURE* ALGORITMA RSA PADA LPPM UIN SUSKA

TUGAS AKHIR

Oleh

M. HANAFI
11551102776

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar sarjana Teknik Informatika
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau di
Pekanbaru, pada tanggal 12 Desember 2019

Pekanbaru, 12 Desember 2019

Mengesahkan,

Dekan,

Ketua Jurusan,

Dr. Drs. Ahmad Darmawi., M. Ag.
NIP. 19660604 199203 1 004

Dr. Elin Haerani, ST., M.Kom
NIP. 19810523 200710 2 003

DEWAN PENGUJI

Ketua	: Iwan Iskandar, M .T.
Pembimbing I	: Pizaini, S.T., M.Kom .
Pembimbing II	: Dr. Alwis Nazir, M.Kom.
Penguji I	: Febi Yanto, M.Kom.
Penguji II	: Muhammad Affandes, M.T.

iii

LEMBAR HAK KEKAYAAN INTELEKTUAL

Tugas akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum dengan ketentuan bahwa hak cipta pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan seizin penulis dan harus disertai dengan kebiasaan ilmiah untuk menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh tugas akhir ini harus memproleh izin dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan yang meminjamkan tugas akhir ini untuk anggotanya diharapkan untuk mengisi nama, tanda peminjaman dan tanggal peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan pada suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali secara tertulis diacu dalam naskah ini dan disebutkan didalam daftar pustaka.

Pekanbaru, 12 Desember 2019

Yang membuat pernyataan,

M. HANAFI

11551102776

LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Alhamdulillahi Rabbil'alamiiin

Tidak ada kata yang bisa diucapkan selain kata syukur kepada

Allah 'Azza Wa Jalla

Sholawat serta salam untuk Rasulallah

Muhammad Shalallahu 'Alaihi Wa Sallam

Serta ucapan terimakasih pada ayah dan ibu tercinta, atas tetesan keringat, motivasi, saran dan nasihatnya. Sehingga laporan Tugas Akhir ini dapat terselesaikan.

Kupersembahkan karya sederhana ini untuk

Ayah, Ibu, Kakak, dan Adik

Dan bagi para pembaca yang membaca.

Terimakasih

APLIKASI PENGAJUAN SURAT MENGGUNAKAN *DIGITAL SIGNATURE* ALGORITMA RSA PADA LPPM UIN SUSKA

M. HANAFI
11551102776

Tanggal Sidang : 12 Desember 2019

Priode Wisuda : September 2020

Jurusan Teknik Informatika

Fakultas Sains dan Teknologi

Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

LPPM UIN SUSKA merupakan lembaga mengelola segala aspek yang berkaitan dengan penelitian dan pengabdian civitas akademika pada UIN SUSKA. Pada masa penelitian pengajuan pembuatan surat penelitian dan pengabdian pada LPPM UIN SUSKA bisa mencapai puluhan dalam satu hari. Sehingga, apabila LPPM tidak berada dikantor atau sedang dinas ke luar kota, akan terjadi penumpukan surat yang harus ditandatangani oleh LPPM UIN SUSKA dan surat-surat tersebut akan terbengkalai sampai LPPM UIN SUSKA kembali masuk bekerja. Maka berdasarkan hasil penelitian yang telah dilakukan solusi nya adalah dengan menggunakan aplikasi pengajuan surat yang menggunakan *digital signature* dalam penandatanganan dokumen. *Digital signature* yang digunakan adalah *digital signature* yang diproses menggunakan algoritma RSA. Aplikasi yang telah dibangun memungkinkan dosen untuk mengajukan permohonan surat secara *online* dan LPPM UIN SUSKA dapat menandatangani dokumen melalui aplikasi menggunakan *digital signature* yang dapat membuktikan keaslian sebuah dokumen.

Kata Kunci: Dekripsi, *Digital Signature*, Enkripsi, *Message Digest*, Verifikasi

APPLICATION OF SUBMISSION LETTER USING RSA ALGORITHM DIGITAL SIGNATURE ON LPPM UIN SUSKA

M. HANAFI
1151102776

Session Date : Desember 12, 2019

Graduation Prize : September 2020

Informatics Engineering

Faculty of Science and Technology

Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRACT

LPPM UIN SUSKA is an institution that manages all aspects related to research and academic community service at UIN SUSKA. During the research period, the submission of research and service letters to the LPPM UIN SUSKA could reach tens in one day. So, if the Chairperson of the LPPM is not in the office or is on duty outside the city, a buildup of letters will have to be signed by the Chairperson of LPPM UIN SUSKA and the letters will be neglected until the Chairperson of LPPM UIN SUSKA returns to work. So based on the results of research the solution has been done is to use a letter submission application that uses digital signatures in signing documents. The application that has been built allows the lecturer to submit a letter request online and the Chairperson of LPPM UIN SUSKA can sign documents through the application using a digital signature that can prove the authenticity of a document.

Keywords: Decryption, Digital Signature, Encryption, Message digest, Verification

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Assalamu'alaikum wa rahmatullahi wa barakaatuh

Alhamdulillahi rabbil'alamin, ucapan syukur kepada Allah 'Azza Wa Jalla yang senantiasa memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penelitian dan penulisan laporan tugas akhir ini yang berjudul **"APLIKASI PENGAJUAN SURAT MENGGUNAKAN *DIGITAL SIGNATURE* PADA LPPM UIN SUSKA".** Shalawat dan salam kepada Rasulallah Muhammad Shalallahu 'Alaihi Wa Sallam, yang telah membimbing kita ke jalan yang lurus dan penuh cahaya serta ridha dari Allah 'Azza Wa Jalla, sehingga kita dapat merasakan sains dan teknologi yang memudahkan aktivitas dan ibadah kita sehari-hari.

Laporan tugas akhir ini disusun sebagai salah satu syarat untuk mendapatkan gelar Sarjana Teknik pada jurusan Teknik Informatika Universitas Islam Negeri Sultan Syarif Kasim Riau. Selama proses dalam menyelesaikan tugas akhir ini, telah mendapatkan bantuan, bimbingan, dukungan, serta motivasi baik secara langsung atau tidak langsung. Untuk itu, pada kesempatan ini penulis ingin menyampaikan ucapan terimakasih kepada:

1. Bapak Prof. DR. KH. Akhmad Mujahidin, S.Ag., M.Ag., selaku Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Bapak Dr. Ahmad Darmawi, M.Ag., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
3. Ibu Dr. Elin Hearani, ST., M.Kom, selaku Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
4. Bapak Febi Yanto, M.Kom, selaku Pembimbing Akademik dan sekaligus Penguji I Tugas Akhir.
5. Bapak Pizaini, S.T., M.Kom, selaku Pembimbing I Tugas Akhir.

6. Bapak Dr.Alwis Nazir, M.Kom, selaku Pembimbing II Tugas Akhir.
7. Bapak Muhammad Affandes, MT, selaku Penguji II Tugas Akhir.
8. Seluruh Dosen Teknik Informatika yang telah memberikan ilmu dan bimbingan yang bermanfaat untuk kami.
9. Ayah Tarmizi, dan Ibu Nurlaili yang telah memberikan motivasi, saran, kasih sayang dan curahan keringat mereka, sehingga laporan ini dapat diselesaikan. Dan Kak Lisa Ramadhani, Bang Muhammad Ibnu, Riski Wahyudi, Asmita Meilani, Muhammad Haikal Saputra atas doa dan motivasinya.
10. Sahabat-sahabat sholeh yang telah memberi doa, motivasi dan saling membantu selama masa perkuliahan.
11. Teman-teman TIF D 2015 yang tidak bisa penulis sebutkan namanya satu-persatu yang telah saling membantu selama masa perkuliahan, memotivasi dan saling mendoakan.
12. Semua Pihak yang turut memberikan doa, bantuan dan motivasinya baik secara langsung atau tidak langsung.

Semoga laporan Tugas Akhir ini dapat bermanfaat bagi para pembacanya. Mohon maaf apabila dalam penulisan Tugas Akhir ini terdapat kesalahan dalam penulisan atau bahasa dalam pembahasan. Apabila ada kritik dan saran untuk laporan Tugas Akhir ini dapat disampaikan melalui alamat email *m.hanafi12@students.uin-suska.ac.id*. Selamat membaca dan semoga bermanfaat.

wassalamu'alaikum wa rahmatullahi wa barakaatuh

Pekanbaru, 12 Desember 2019

M. HANAFI

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR RUMUS

DAFTAR SIMBOL

Keterangan notasi simbol *flowchart* :

Terminator : Simbol terminator (mulai / selesai) merupakan simbol yang menunjukkan permulaan dan akhir dari proses

Proses : Simbol yang digunakan untuk melakukan pemrosesan data baik oleh user maupun komputer (sistem).

Verifikasi : Simbol yang digunakan untuk memutuskan apakah valid atau tidak validnya suatu kejadian.

Data : Simbol yang digunakan untuk mendeskripsikan data yang digunakan

BAB I
PENDAHULUAN

1.1 Latar Belakang

Tanda tangan pada suatu dokumen berfungsi sebagai bukti keabsahan dokumen bahwa dokumen telah diketahui dan disetujui oleh penandatangan. Tanda tangan sering digunakan untuk mengesahkan dokumen perizinan, perjanjian, ijazah dan dokumen penting lainnya.

Pada bidang kriptografi terdapat mekanisme penandatanganan yang dapat menggantikan tanda tangan konvensional atau tanda tangan tertulis yaitu *digital signature. Digital signature* bukanlah tanda tangan basah yang dipindai lalu disematkan pada dokumen, *digital signature* adalah hasil enkripsi isi dokumen yang diringkas menggunakan fungsi *hash* lalu disematkan pada dokumen. Jika isi tanda tangan tertulis bergantung pada siapa yang menandatangani, berbeda hal nya dengan *digital signature* yang isi tanda tangan nya bergantung pada isi dokumen, sehingga tanda tangan yang dihasilkan oleh *digital signature* akan berbeda pada setiap dokumen (Ihwani, 2016).

Proses penandatangan menggunakan *digital signature* diawali dengan meringkas isi dokumen menggunakan fungsi *hash*, lalu hasil ringkasan tersebut dienkripsi menggunakan kunci privat pengirim, dan pada proses akhir, hasil enkripsi disematkan pada dokumen. Untuk proses verifikasi, *digital signature* yang telah disematkan dideskripsi menggunakan kunci publik penerima lalu dibandingkan dengan hasil ringkasan isi dokumen yang diringkas menggunakan fungsi *hash*. Apabila sama, maka dokumen tersebut adalah dokumen yang asli. Salah satu algoritma enkripsi yang umum dipakai dalam penerapan *digital signature* adalah algoritma RSA (Rionaldy, 2017).

RSA adalah algoritma kunci publik yang menggunakan kunci berbeda pada proses enkripsi dan deskripsi. Algoritma ini dikembangkan oleh Ron Rivest, Adi Shamir dan Len Adleman. Algoritma RSA adalah algoritma pertama yang diterapkan pada *digital signature*. Algoritma dianggap sebagai algoritma yang sangat aman karena pada algoritma ini terdapat proses pemfaktoran yang besar pada proses enkripsi dan enkripsi (Kurniawan, 2004).

Penerapan *digital signature* di Indonesia sudah mulai diberlakukan oleh Kementrian Komunikasi dan Informatika atau Kominfo, tidak hanya perusahaan swasta, Kominfo juga mulai memberlakukan tanda tangan digital untuk perizinan di berbagai Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu (DPMPTSP) diseluruh Indonesia (KOMINFO, 2018).

Semakin berkembangnya *digital signature* di Indonesia semakin berkembang pula penelitian yang berkaitan dengan *digital signature* diantara nya :

1. Penerapan Tanda Tangan Digital pada Sistem Pemerintahan guna mendukung e-government (Nugraha, 2016). Penelitian ini membahas tentang penerapan *digital signature* pada instansi pemerintahan untuk membantu mengamankan dokumen dan menjada integritas dokumen elektronik.
2. Pengamanan Sertifikat Tanah Digital Menggunakan *Digital Signature* SHA-512 dan RSA (Refialy, 2015). Penelitian yang dilatarbelakangi rentannya sertifikat tanah terhadap penggandaan dan modifikasi yang tidak sah ini menerapkan fungsi *hash* SHA-512 untuk pengamanan menggunakan *digital signature* pada dokumen sertifikat tanah.
3. Penerapan *Digital Signature* Dengan Algoritam SHA-1 Pada Surat Legalisasi Ijazah dan Transkrip Nilai Mahasiswa(Wahyuni, 2014). Penelitian ini dilakukan untuk menghindari pemalsuan dokumen ijazah dan transkrip nilai dengan membuat aplikasi *digital signature* algoritma SHA-1.
4. Implementasi RSA sebagai *Digital Signature* pada Publikasi Arsip Elektronik Berbasis Web (Rionaldy, 2017). Penelitian ini bertujuan untuk membangun sebuah sistem pengamanan arsip surat dengan menggunakan digital signature

RSA. Kesimpulan dari penelitian sistem yang dibangun dapat memverifikasi keaslian dari arsip surat.

Berdasarkankan uraian diatas peneliti bermaksud untuk merancang dan membangun Aplikasi *Digital Signature* Algoritma RSA pada LPPM UIN SUSKA. LPPM UIN SUSKA yang merupakan singkatan dari Lembaga Penelitian dan Pengabdian kepada Masyarakat Universitas Islam Negeri Sultan Syarif Kasim adalah lembaga yang memfasilitasi dan melayani dosen di UIN SUSKA Riau dalam melakukan penelitian serta pengabdian kepada masyarakat. Salah satu layanan yang diberikan LPPM UIN SUSKA adalah layanan pembuatan surat izin penelitian dan pengabdian.

Aplikasi *digital signature* yang akan dibangun akan berjalan sesuai dengan layanan pembuatan surat izin penelitian dan pengabdian pada LPPM UIN SUSKA. Dosen dapat mengajukan permohonan pembuatan surat izin secara online, secara otomatis surat akan langsung masuk ke akun LPPM, LPPM dapat menandatangani surat secara digital menggunakan *digital signature*. Setelah surat ditandangani secara digital, secara otomatis surat akan dapat diunduh oleh dosen dan dosen juga dapat melakukan verifikasi pada dokumen surat yang telah ditandatangani oleh LPPM UIN SUSKA melalui aplikasi yang akan dibangun.

1.2 Rumusan Masalah

Berdasarkan uraian yang telah dijelaskan pada latar belakang latar belakang, maka diperoleh rumusan masalah yaitu bagaimana membangun Aplikasi *Digital Signature* Algoritma RSA pada LPPM UIN SUSKA.

1.3 Batasan Masalah

Batasan masalah dibutuhkan untuk menentukan ruang lingkup pembahasan suatu penelitian, mengingat permasalahan yang ada begitu luas serta keterbatasan pengetahuan yang dimiliki. Permasalahan yang akan dibahas pada Tugas Akhir ini adalah sebagai berikut:.

1. Penelitiaan ini tidak membahas performansi dari algoritma RSA pada *digital signature.*

2. Dokumen surat yang digunakan pada penelitian ini adalah dokumen yang berekstensi *.pdf*
3. Aplikasi yang dibangun adalah aplikasi *digital signature* berbasis web
4. Surat izin yang dapat diajuakan hanya surat izin penelitian, surat izin pengabdian, dan surat izin *focus group discussion*

1.4 Tujuan Penelitian

Tujuan dari penelitian tugas akhir ini adalah sebagai berikut:

1. Mengimplementasikan *digital signature* RSA pada LPPM UIN SUSKA
2. Memberikan kemudahan dalam proses pelayanan pembuatan surat izin penelitian dan pengabdian pada LPPM UIN SUSKA yang didukung dengan mengimplementasikan *digital signature.*

1.5 Sistematika Penulisan

Laporan penelitian ini memiliki enam bab yang terdiri dari beberapa sub bab yaitu:

BAB I PENDAHULUAN

Pada bab ini dijelasakan latar belakang dari penelitian, batasan masalah penelitian, rumusan masalah, tujuan penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini peneliti menjelaskan teori singkat tentang hal-hal yang berhub-ungan dengan judul, model pengembangan aplikasi serta tentang teori-teori yang mendukung pembuatan aplikasi *digital signature* algoritma RSA pada LPPM UIN SUSKA

BAB III METODOLOGI PENELITIAN

Pada bab ini berisi tentang beberapa rangkaian tahapan dalam pembuatan aplikasi, mulai dari melakukan pengumpulan data, analisis dan perancangan, hingga tahap implementasi dan pengujian yang digunakan.

BAB IV ANALISIS DAN PERANCANGAN

Pada bab ini menjelaskan tentang analisis dan rancangan dari aplikasi yang akan dibangun.

BAB V IMPLEMENTASI DAN PENGUJIAN

Pada bab ini berisi tentang hasil implementasi dari analisis dan perancangan yang telah dibuat sebelumnya, yaitu meliputi implementasi basis data, implementasi metode yang digunakan dan implementasi form-form antar muka aplikasi.

BAB VI PENUTUP

Pada bab ini berisi hasil penelitian yaitu kesimpulan dan saran yang dapat dijadikan referensi untuk pengembangan penelitian selanjutnya

BAB II
LANDASAN TEORI

2.1 Kriptografi

Kriptografi merupakan ilmu atau seni untuk mengamankan pesan. Kriptografi berasal dari dua kata kripto dan graphia yang merupakan kata dari bahasa yunani yang memiliki arti rahasia dan tulisan. Kriptografi sudah telah digunakan oleh orang mesir 4000 tahun yang lalu untuk mengamankan pesan dari pihak musuh untuk dikirim kepasukan militer yang berada dilapangan (Kromodimoeljo, 2010).

Dahulu nya kriptografi hanya dipelajari oleh pasukan militer seperti agen Keamanan Israel, Inggris, Uni Soviet dan Negara-negara lainnya yang menggunakan untuk menjaga kerahasiaan komunikasi mereka agar tidak diketahui oleh pihak luar. Namun, pada tiga puluh tahun yang lalu kriptografi mulai digunakan oleh individu untuk mengamankan informasi keluarga, pekerjaan, bisnis, dan lainnya (Ariyus, 2006).

2.2 Algoritma Kunci Publik

Algoritma kunci publik atau yang biasa disebut algoritma asimetris yang merupakan algoritma yang memiliki kunci yang berbeda untuk enkripsi dan deskripsi. Terdapat dua kunci pada algoritma kunci publik yaitu kunci publik dan kunci privat. Kunci privat adalah kunci yang hanya dapat diketahui oleh orang tertentu saja yang memiliki kuasa terhadap kunci privat sedangkan kunci publik adalah kunci yang dapat disebarkan kepada orang lain. Pada Algoritma kunci publik jika pesan dienkripsi menggunakan kunci privat maka untuk mendeskripsi pesan hanya dapat menggunkan kunci publik begitu juga sebaliknya (Kurniawan, 2004).

2.3 *Digital signature*

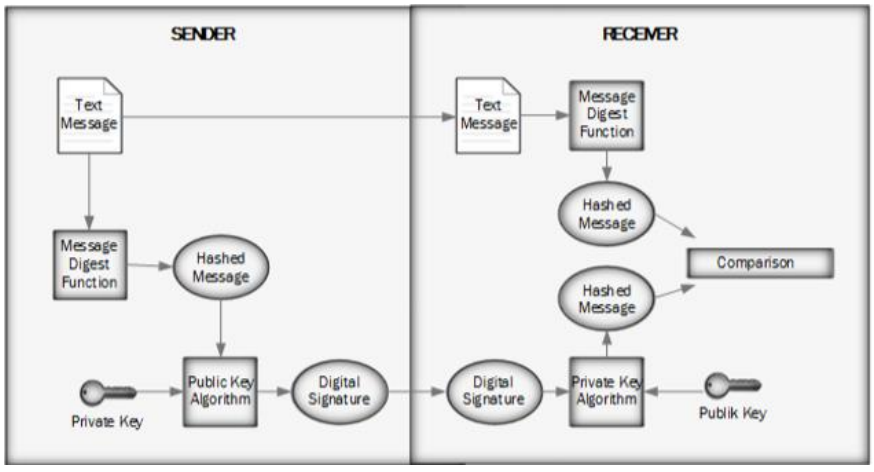
Digital signature merupakan kumpulan bit yang yang dapat melakukan fungsi elekronik yang menggunakan fungsi *hash* kemudian dienkripsi dengan algoritma kunci publik (Andi, 2003).

Sifat dari *digital signature* diantaranya:

1. Otentik, jaminan keaslian pesan atau integritas pesan, pesan sulit untuk dimanimpulasi oleh orang lain.
2. Hanya berlaku untuk satu kali pengiriman pesan, *digital signature* hanya dapat digunakan pada dokumen yang memiliki *digital signature*, tidak dapat dipindahkan ke dokumen lain.
3. *Digital signature* dapat diperiksa keabsahan nya oleh penerima pesan.

Proses *digital signature* diawali dengan mengubah isi dokumen menjadi *message digest* menggunakan fungsi *hash*, selanjutnya *message digest* dienkripsi menggunakan kunci privat, hasil enkripsi inilah yang kemudian disebut sebagai *digital signature*, kemudian hasil enkripsi disematkan pada dokumen. Untuk proses verifikasi *digital signature*, *digital signature* dideskripsi menggunakan kunci publik dan akan menghasilkan *message digest*. *message digest* tersebut dibandingkan dengan *message digest* dari dokumen yang asli. Apabila nilai *message digest* nya sama maka pesan tersebut berasal dari pengirim yang sebenarnya (Kurniawan, 2004).

Gambar 2.1 memperlihatkan proses penandatanganan menggunakan *digital signature* dan proses verifikasi *digital signature*



Gambar 2.1 Proses *Digital Signature* Pada Dokumen

Keotentikan pesan dapat dijelaskan sebagai berikut:

a) Apabila *message digest* pada pesan yang telah ditandatangani berbeda dengan *message digest* pada pesan yang semula maka pesan tersebut tidak asli atau sudah mengalami perubahan.
b) Jika *digital signature* tidak dapat dideskripsi menggunakan kunci publik, maka pesan tersebut tidak berasal dari pengirim yang sebenarnya, hal ini karena kunci privat pengirim pesan tidak berkoreponden dengan kunci publik yang dimiliki penerima.
c) Jika message digest yang dihasilkan pada proses deskripsi *digital signature* sama dengan *message digest* pesan semula maka pesan tersebut asli dan berasal dari pengirim yang sebenarnya (Munir, 2006).

2.4 Algoritma RSA

RSA adalah algoritma kunci asimetri yang menggunakan kunci berbeda untuk enkripsi dan deskripsi. Algoritma ini dikembangkan oleh tiga orang yaitu Ron Rivest, Adi Shamir dan Len Adleman dari MIT (*Massachusetts Institute of Technology*) pada tahun 1997. Nama RSA berasal dari singkatan nama mereka (Kurniawan, 2004).

Pemfaktoran yang besar pada proses enkripsi dan dekripsi merupakan alasan mengapa algoritma ini dianggap aman. Pada RSA kunci dibangkitkan dengan memilih dua buah bilangan prima yang dipilih secara acak. Algoritma ini mengenkripsi pesan dengan membagi plaintext menjadi blok-blok dan setiap blok diberikan nilai bilangan biner dengan simbol n, plaintext blok M dan *chipertext* blok C. Pesan M kemudian dibagi menjadi blok-blok numerik yang nilainya lebih kecil dari pada nilai n, apabila panjang bilangan prima lebih dari 200 digit dan dan untuk menjaga agar pesan tetap kurang dari nilai n, pada bagian kiri bilangan dapat ditambahkan beberapa bit 0 (Ariyus, 2006).

Ada 3 tahapan dalam penggunaan RSA, yaitu: pemasangan kunci, enkripsi, dan deskripsi.

1. Pembangkitan kunci

   Algoritma pembangkitan kunci mengambil sebuah masukan sebagai parameter *n* dan sebuah parameter tambahan *b*. Algoritma ini membangkitkan pasangan *public key* dan *private key* RSA dengan ketentuan sebagai berikut:

   a. Bangkitkan 2 buah bilangan prima yaitu *p* dan *q*
   b. Hitung n = p x q.
   c. Hitung $\phi(n) = (p-1) \times (q-1)$.
   d. Pilih e yang nilai nya relatif prima terhadap $\phi(n)$.
   e. Tentukan kunci privat d dengan persamaan $d = (1 + a*\phi(n))/e$, dengan a adalah bilangan bulat yang dapat memenuhi.
   f. Sehingga didapat pasangan kunci publik (e,n) dan kunci privat (d,n).

2. Enkripsi

   Pada proses ini kunci privat (e,n) akan digunakan. Untuk mengenkripsi *plaintext* menjadi *ciphertext* dapat dilakukan dengan cara berikut:

$$C = M^e \, Mod \, n \qquad (2.1)$$

3. Dekripsi

   Untuk mendekripsi *ciphertext* C digunakan *private key* (d,n), dengan cara berikut :

$$M = C^d \, Mod \, n \qquad (2.2)$$

2.5 Algoritma SHA

Algoritma SHA (*Secure Hash Algorithm*) merupakan algoritma kriptografi satu arah hasil rancangan *National Security Agency* (NSA). Pada tahun 1993 NIST mempublikasikan algoritma ini yang disebut SHA-0 sebagai Federal Information Processing (FIPS) , dua tahun kemudian NIST kembali mempublikasikan generasi

Selanjutnya yaitu SHA-1 . Pada tahun 2002 dipublikasikan empat versi lainnya yaitu SHA-224, SHA-256, SHA-384, SHA-512, yang disebut sebagai SHA-2 (Refialy, 2015).

Secara komputasi pada algoritma SHA pesan yang telah menjadi *message digest* tidak ditemukan kembali sehingga SHA ini dinyatakan sebagai algoritma yang aman. Setiap pesan akan menghasilkan *message digest* yang berbeda. Algoritma SHA memiliki perbedaan pada ukuran tiap blok, *word* dari data yang digunakan pada saat proses *hashing*, panjang pesan yang diproses tergantung pada algoritma yang dipakai (Kromodimoeljo, 2010).

2.6 Landasan Hukum *Digital signature*

Berdasarkan Pasal 11 Ayat 1 Undang-Undang 11/2008 tentang ITE yang berbunyi :

Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

a. data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
b. data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;
c. segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
d. segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
e. terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya; dan
f. terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

2.7 Penelitian Terkait

Berikut ini merupakan penelitian terkait tentang *digital signature* yang disajikan dalam tabel:

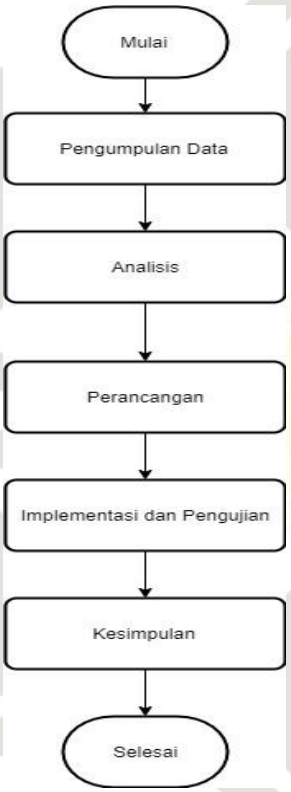
Tabel 2.1 Penelitian Terkait

No.	Penulis	Judul	Deskripsi
1.	(Agung Nugraha, 2016)	Penerapan tanda tangan elektronik pada sistem pemerintahan guna mendukung *e-government*	Penelitian ini membahas tentang penerapan *digital signature* pada instansi pemerintahan untuk membantu mengamankan dokumen dan menjada integritas dokumen elektronik.
2.	(Leonardo Refialy, Eko Sediyono, & Adi Setiawan, 2015)	Pengamanan sertifikat tanah digital menggunakan *digital signature* SHA-512 dan RSA	Penelitian yang dilatarbelakangi rentannya sertifikat tanah terhadap penggandaan dan modifikasi yang tidak sah ini menerapkan fungsi *hash* SHA-512 untuk pengamanan menggunakan *digital signature* pada dokumen sertifikat tanah. Hasil dari penelitian adalah sertifikat tanah berhasil ditandatangani dengan *digital signature* tanpa perubahan yang signifikan pada dokumen.
3.	(Sri Wahyuni,	Penerapan *Digital*	Penelitian ini dilakukan un-

	2016	*Signature* Dengan Algoritam SHA-1 Pada Surat Legalisasi Ijazah dan Transkrip Nilai Mahasiswa	tuk menghindari pemalsuan dokumen ijazah dan transkrip nilai dengan membuat aplikasi *digital signature* algoritma SHA-1.
	(Muhammad Ihwani, 2016)	Model keamanan informasi berbasis *digital signature* dengan algoritma RSA	Kesimpulan pada penelitian algoritma RSA dapat menjaga keamanan dan kerahasiaan file dan pesan jika diterapkan pada *digital signature*
5.	(Rizqi Rionaldy, 2016)	Implementasi RSA sebagai *Digital Signature* pada Publikasi Arsip Elektronik Berbasis Web	Penelitian ini bertujuan untuk membangun sebuah sistem pengamanan arsip surat dengan menggunakan *digital signature* RSA. Kesimpulan dari penelitian sistem yang dibangun dapat memverifikasi keaslian dari arsip surat

BAB III
METODOLOGI PENELITIAN

Suatu penelitian diperlukan metode pendekatan atau penyelesaian untuk melaksanakan suatu penelitian agar penelitian berjalan dengan lancar dan sesuai dengan tujuan yang telah ditentukan sehingga tercapai hasil yang baik. Berikut ini adalah tahapan penelitian dalam menyelesaikan tugas akhir pada Gambar 3.1:



Gambar 3.1 Tahapan Penelitian

3.1 Pengumpulan Data

Pada tahap ini peneliti melakukan pengumpulan data untuk mempermudah melakukan tahap selanjutnya yaitu tahap analisis memalui berbagai cari meliputi, wawancara dan studi literatur yang berkaitan dengan penerapan *digital signature* menggunakan algoritma RSA pada dokumen seperti konsep *digital signature*, cara kerja Algoritma RSA pada *digital signature*, fungsi *hash* satu arah SHA dan implementasi *digital signature* pada bahasa pemograman.

3.2 Analisis

Setelah melakukan tahap pengumpulan data maka yang dilakukan selanjutnya adalah melakukan proses Analisis. Adapun proses analisis yang dilakukan meliputi

1. Melakukan analisa bagan proses aplikasi yang akan dibangun agar sesuai dengan proses yang berjalan pada LPPM UIN SUSKA.
2. Melakukan analisa terhadap proses yang berjalan pada *digital signature*, ada dua proses pada *digital signature* yaitu proses penandatanganan dan proses verifikasi

3.3 Perancangan

Tahap ini merupakan tahap perancangan aplikasi pada tahap ini akan dilakukan proses pembuatan rancangan aplikasi meliputi perancangan antarmuka aplikasi dan perancangan *digital signature* berdasarkan kebutuhan untuk mengimplementasikan *digital signature* menggunakan algoritma RSA.

3.4 Implementasi dan Pengujian

Tahap ini merupakan tahap dimana aplikasi yang dibuat siap untuk diimplementasikan pada LPPM UIN SUSKA dan dilakukan pengujian.

3.4.1 Implementasi

Pada tahap ini akan dilakukan proses implementasi hasil rancangan meliputi implementasi pemodelan UML, implementasi *digital signature* RSA, dan rancangan antarmuka kedalam bahasa pemograman. Untuk melakukan implementasi terhadap aplikasi ini maka dibutuhkan perangkat yang dapat mendukung proses implementasi, perangkat tersebut berupa perangkat lunak dan perangkat keras. Adapun Perangkat keras yang dibutuhkan antara lain yaitu:

1. *Processor* : Core i7
2. *Memory* : 8 GB
3. HDD : 500 GB

Perangkat lunak yang dibutuhkan:

1. *Platform* : Windows
2. Bahasa Pemograman : PHP
3. DBMS : MySQL
4. *Web server* : Apache
5. *Browser* : Google Chrome

3.4.2 Pengujian

Pada tahap pengujian dilakukan pengujian terhadap aplikasi untuk menguji fungsi-fungsi yang ada pada aplikasi apakah berjalan sesuai dengan yang diharapkan. Pengujian akan dilakukan terhadap aplikasi adalah pengujian penandatanganan dan pengujian verifikasi dokumen.

3.5 Kesimpulan dan Saran

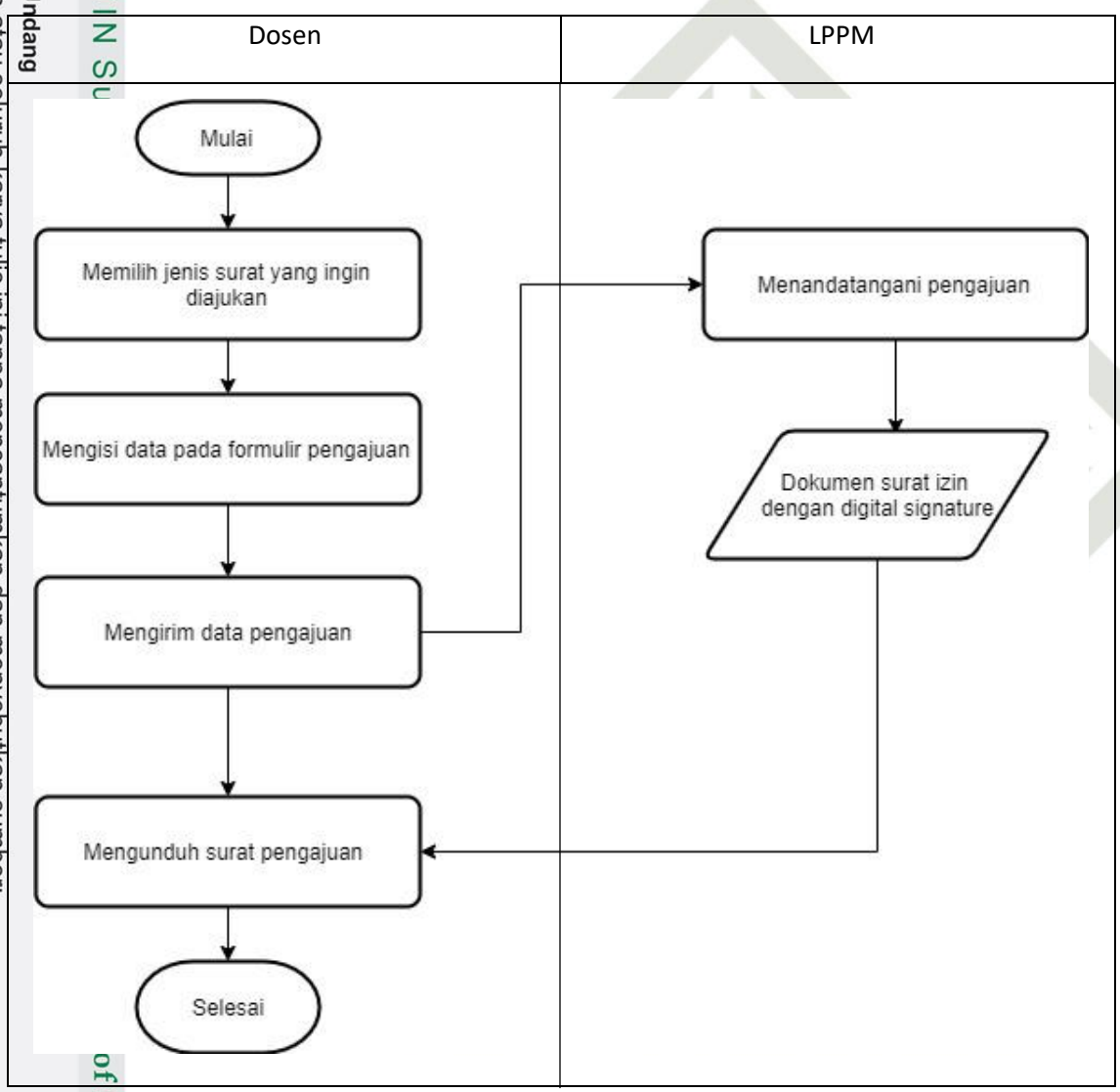
Kesimpulan berisi hasil dari penelitian yang dilakukan dalam merancang dan membangun Aplikasi *Digital signature* Algoritma RSA pada LPPM UIN SUSKA dan saran berisi anjuran-anjuran yang dapat digunakan untuk pengembangan penilitian selanjutnya.

BAB IV

ANALISIS DAN PERANCANGAN

4.1 Analisis Aplikasi

Aplikasi pengajuan surat menggunakan *digital signature* yang akan dibangun memiliki proses sebagai berikut:



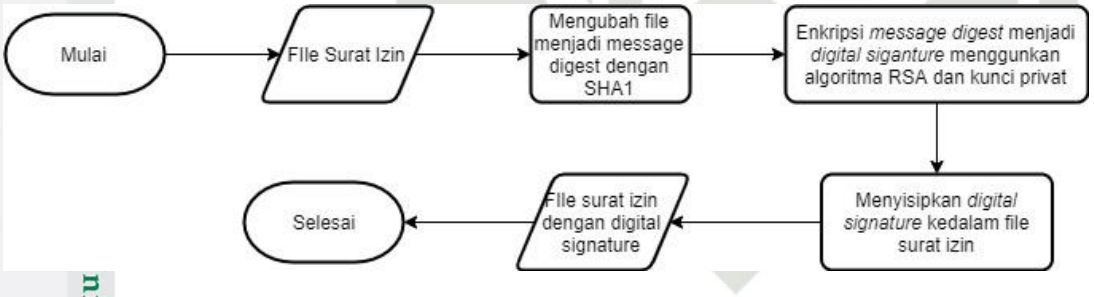
Gambar 4.1 Flowchart Aplikasi Pengajuan Surat Izin Menggunakan *Digital Signature.*

1. Dosen memilih jenis surat yang ingin diajukan, terdapat 3 jenis surat yang dapat diajukan yaitu surat izin penelitian, surat izin pengabdian, surat izin *focus group discussion.*
2. Dosen mengisi formulir pengajuan, lalu aplikasi akan secara otomatis membuat dokumen sesuai dengan pengajuan.
3. LPPM menyetujui pengajuan dan aplikasi akan memproses dokumen pengaajuan sehingga dokumen memiliki *digital signature.*
4. Dosen dapat mengunduh dokumen yang sudah memiliki *digital signature.*

4.2 Analisis Penandatanganan Menggunakan *Digital Signature*

Digital Signature yang digunakan pada aplikasi adalah *digital signature* yang menggunakan *hash* SHA dan Algoritma RSA untuk proses penandatanganan. Proses penandatanganan menggunakan *digital signature* dimulai dengan mengubah file dokumen berekstensi .pdf menjadi *messeage digest* mengunakan SHA, lalu *message digest* tersebut akan di enkripsi menggunakan algoritma RSA. Hasil enkripsi kemudian disematkan pada dokumen .pdf.

Berikut merupakan flowcart dari proses penandatanganan:



Gambar 4. 2 Flowchart Proses Penandatanganan Dokumen Surat Izin Menggunakan *Digital Signature*

4.3 Analisis SHA

Tahapan awal yang dilalui ketika proses penandatangan dokumen surat izin adalah dengan merubah e-dokumen surat izin menjadi *message digest* dengan menggunakan fungsi *hash* SHA. Fungsi *hash* SHA yang digunankan pada aplikasi ini

adalah SHA-1 dimana pada SHA-1 *message digest* yang dihasilkan adalah berjumlah 128 bit.

Proses pengubahan e-dokumen menjadi *message digest* dimulai dengan membagi nya menjadi blok-blok yang memiliki panjang 512 bit setiap bloknya. Setiap blok teridiri dari 16 *word* dan setiap *word* terdiri dari 32 bit. Blok yang sudah dibagi-bagi kemudian diproses bersama dengan penyangga *message digest* yang berjumlah 5 penyangga yang masing-masing penyangga memiliki panjang 32 bit. Hasil proses kemudian digabungkan sehingga menjadi *message digest* dengan panjang 128 bit.

Berikut adalah contoh cara kerja SHA-1:

1. Pesan Masukan yaitu “lppm”.
2. Ubah pesan menjadi biner sehingga menjadi bilangan biner, sehinnga menjadi seperti ini 01101100011100000111000001101l0.
3. Tambahkan bit “1” pada akhir pesan
4. Tambahkan bit “0” sehingga panjang pesan menjadi 448. Karena panjang pesan adalah 33 bit maka bit 0 yang ditambahkan ada 415 bit.
5. Tambahkan 64 bit yang mempresentasikan panjang awal dari pesan. Panjang pesan semula adalah 32 bit maka bit yang ditambahkan adalah (0…...001000000).
6. Inisialisasi penyangga MD. SHA membutuhkan 5 buah penyangga yang masing panjang penyangga adalah 32 bit. Penyangga SHA adalah sebagai berikut :

   A=67452301

   B=EFCDAB89

   C=98BADCFE

   D=10325476

   E=C3D2E1F0
7. Bagi pesan menjadi 16 buah blok dengan panjang setiap blok adalah 32 bit. Berikut adalah 16 blok pesan yang telah dibagi

   W[0] = 01101100011100000110000001101101

   W[1] =10000000000000000000000000000000

   W[2] = 00000000000000000000000000000000

   W[3] = 00000000000000000000000000000000

W[4] = 00000000000000000000000000000000
W[5] = 00000000000000000000000000000000
W[6] = 00000000000000000000000000000000
W[7] = 00000000000000000000000000000000
W[8] = 00000000000000000000000000000000
W[9] = 00000000000000000000000000000000
W[10] = 00000000000000000000000000000000
W[11] = 00000000000000000000000000000000
W[12] = 00000000000000000000000000000000
W[13] = 00000000000000000000000000000000
W[14] = 00000000000000000000000000000000
W[15] = 00000000000000000000000000100000

8. Setiap blok diproses bersama dengan penyangga sehingga menghasilkan keluaran 128 bit dan proses ini disebut H_{SHA}. Proses ini terdiri dari 80 putaran dan masing-masing putaran menggunakan bilangan penambah, yaitu:

   Putaran 0-19: Kt =5A827999

   Putaran 20-39: Kt=6ED9BA1

   Putaran 40-59: Kt=8F1BBCDC

   Putaran 60-79: Kt=CA62C1D6

9. Operasi dari 80 putaran tersebut dapat dijabarkan pada algoritma berikut:

   For t ← 0 to 79 do

   TEMP ← (a <<< 5) + ft (b,c,d) + e + Wt + Kt)

   e ← d

   d ← c

   c ← b <<< 30

   b ← a

   a ← TEMP end for

   (Dalam hal ini, <<< menyatakan operasi pergeseran *circular left shift* (CLSs)).

10. Berikut adalah operasi pada putaran pertama

A = CLS5(A) + F(b,c,d) + E + W[1] + K[1]

=11101000101001000110000000101100

+10011000101110101101110011111110

+11000011110100101110000111110000

+11011000111000001110000001101101

+10110101000001001111001100110001

= 00001100001001010000100100100000

= 0C250920

B = A

= 67452301

C = CLS30(B)

= 01111011111100110110101011011011111110

= 7BF36AE2

D = C

= 98BADCFE

E = D

= 10325476

11. Sehingga pada putaran pertama didapatkan hasil sebagai berikut

A=0C250920

B = 67452301

C = 7BF36AE2

D = 98BADCFE

E = 10325476

12. Berikut adalah hasil dari 80 putaran pada SHA1:

	A	B	C	D	E
putaran 1:	0c250920	67452301	7bf36ae2	98badcfe	10325476
putaran 2:	6b51f10e	0c250920	59d148c0	7bf36ae2	98badcfe
putaran 3:	d94ee326	6b51f10e	03094248	59d148c0	7bf36ae2

putaran	4:	13d3921e	d94ee326	9ad47c43	03094248	59d148c0
putaran	5:	c90b6665	13d3921e	b653b8c9	9ad47c43	03094248
putaran	6:	195084e3	c90b6665	84f4e487	b653b8c9	9ad47c43
putaran	7:	d5b88ecc	195084e3	7242d999	84f4e487	b653b8c9
putaran	8:	5cccec81	d5b88ecc	c6542138	7242d999	84f4e487
putaran	9:	5f673f64	5cccec81	356e23b3	c6542138	7242d999
putaran	10:	50096176	5f673f64	57333b20	356e23b3	c6542138
putaran	11:	992e054e	50096176	17d9cfd9	57333b20	356e23b3
putaran	12:	cceca26f	992e054e	9402585d	17d9cfd9	57333b20
putaran	13:	e61dcd8f	cceca26f	a64b8153	9402585d	17d9cfd9
putaran	14:	ca60d3c1	e61dcd8f	f33b289b	a64b8153	9402585d
putaran	15:	1cfa530a	ca60d3c1	f9877363	f33b289b	a64b8153
putaran	16:	9933d7aa	1cfa530a	729834f0	f9877363	f33b289b
putaran	17:	3eb6a8c2	9933d7aa	873e94c2	729834f0	f9877363
putaran	18:	0e99ba16	3eb6a8c2	a64cf5ea	873e94c2	729834f0
putaran	19:	475ea64c	0e99ba16	8fadaa30	a64cf5ea	873e94c2
putaran	20:	2e258990	475ea64c	83a66e85	8fadaa30	a64cf5ea
putaran	21:	252d768b	2e258990	11d7a993	83a66e85	8fadaa30
putaran	22:	608ab63b	252d768b	0b896264	11d7a993	83a66e85
putaran	23:	a6ce6279	608ab63b	c94b5da2	0b896264	11d7a993
putaran	24:	fcc66ea9	a6ce6279	d822ad8e	c94b5da2	0b896264
putaran	25:	7c9a764e	fcc66ea9	69b3989e	d822ad8e	c94b5da2
putaran	26:	dfd2759f	7c9a764e	7f319baa	69b3989e	d822ad8e
putaran	27:	ab63c2ac	dfd2759f	9f269d93	7f319baa	69b3989e
putaran	28:	84cb4f7a	ab63c2ac	f7f49d67	9f269d93	7f319baa
putaran	29:	d93546a0	84cb4f7a	2ad8f0ab	f7f49d67	9f269d93
putaran	30:	8e908155	d93546a0	a132d3de	2ad8f0ab	f7f49d67
putaran	31:	0284dcf1	8e908155	364d51a8	a132d3de	2ad8f0ab
putaran	32:	20599920	0284dcf1	63a42055	364d51a8	a132d3de
putaran	33:	44efd38d	20599920	40a1373c	63a42055	364d51a8

putaran	34:	467e4540	44efd38d	08166648	40a1373c	63a42055
putaran	35:	e6d76ead	467e4540	513bf4e3	08166648	40a1373c
putaran	36:	70c3d41a	e6d76ead	119f9150	513bf4e3	08166648
putaran	37:	10f8edda	70c3d41a	79b5dbab	119f9150	513bf4e3
putaran	38:	688da6eb	10f8edda	9c30f506	79b5dbab	119f9150
putaran	39:	4eb3242b	688da6eb	843e3b76	9c30f506	79b5dbab
putaran	40:	2f77d658	4eb3242b	da2369ba	843e3b76	9c30f506
putaran	41:	1062822f	2f77d658	d3acc90a	da2369ba	843e3b76
putaran	42:	fad21c56	1062822f	0bddf596	d3acc90a	da2369ba
putaran	43:	43dba8ba	fad21c56	c418a08b	0bddf596	d3acc90a
putaran	44:	6ad80b55	43dba8ba	beb48715	c418a08b	0bddf596
putaran	45:	043b6a40	6ad80b55	90f6ea2e	beb48715	c418a08b
putaran	46:	9596b1e0	043b6a40	5ab602d5	90f6ea2e	beb48715
putaran	47:	55e166fc	9596b1e0	010eda90	5ab602d5	90f6ea2e
putaran	48:	a54d5596	55e166fc	2565ac78	010eda90	5ab602d5
putaran	49:	341cb1c2	a54d5596	157859bf	2565ac78	010eda90
putaran	50:	4034f1cb	341cb1c2	a9535565	157859bf	2565ac78
putaran	51:	60e8550f	4034f1cb	8d072c70	a9535565	157859bf
putaran	52:	25cf39f5	60e8550f	d00d3c72	8d072c70	a9535565
putaran	53:	6bde5373	25cf39f5	d83a1543	d00d3c72	8d072c70
putaran	54:	67fdedb4	6bde5373	4973ce7d	d83a1543	d00d3c72
putaran	55:	a75c5d0d	67fdedb4	daf794dc	4973ce7d	d83a1543
putaran	56:	baf4dd2b	a75c5d0d	19ff7b6d	daf794dc	4973ce7d
putaran	57:	748c5406	baf4dd2b	69d71743	19ff7b6d	daf794dc
putaran	58:	a60dabf5	748c5406	eebd374a	69d71743	19ff7b6d
putaran	59:	66ae9b41	a60dabf5	9d231501	eebd374a	69d71743
putaran	60:	f46755af	66ae9b41	69836afd	9d231501	eebd374a
putaran	61:	6c5c6c32	f46755af	59aba6d0	69836afd	9d231501
putaran	62:	27cf485e	6c5c6c32	fd19d56b	59aba6d0	69836afd
putaran	63:	a32a8e46	27cf485e	9b171b0c	fd19d56b	59aba6d0

putaran	64:	3b733077	a32a8e46	89f3d217	9b171b0c	fd19d56b
putaran	65:	5c403675	3b733077	a8caa391	89f3d217	9b171b0c
putaran	66:	07dff666	5c403675	cedccc1d	a8caa391	89f3d217
putaran	67:	f6e1e212	07dff666	57100d9d	cedccc1d	a8caa391
putaran	68:	9f46dc58	f6e1e212	81f7fd99	57100d9d	cedccc1d
putaran	69:	49cdb1e3	9f46dc58	bdb87884	81f7fd99	57100d9d
putaran	70:	feb3c921	49cdb1e3	27d1b716	bdb87884	81f7fd99
putaran	71:	7af51763	feb3c921	d2736c78	27d1b716	bdb87884
putaran	72:	690b69cf	7af51763	7facf248	d2736c78	27d1b716
putaran	73:	9f2a8462	690b69cf	debd45d8	7facf248	d2736c78
putaran	74:	5105e417	9f2a8462	da42da73	debd45d8	7facf248
putaran	75:	06b157ed	5105e417	a7caa118	da42da73	debd45d8
putaran	76:	b0e8b2ca	06b157ed	d4417905	a7caa118	da42da73
putaran	77:	6984ccd2	b0e8b2ca	41ac55fb	d4417905	a7caa118
putaran	78:	c9252c2f	6984ccd2	ac3a2cb2	41ac55fb	d4417905
putaran	79:	fa7a0193	c9252c2f	9a613334	ac3a2cb2	41ac55fb
putaran	80:	c6b98da9	fa7a0193	f2494b0b	9a613334	ac3a2cb2

13. Tambahkan A, B, C, D, E dengan penyangga.

    A = A[80] + A = 2dfeb0aa

    B = B[80] + B = ea47ad1c

    C = C[80] + C = 8b042809

    D = D[80] + D = aa9387aa

    E = E[80] + E = 700d0ea2

14. Lalu gabungkan hasil penjumlahan tersebut.

    Sehingga didapatlah *message digest* dari “lppm” adalah sebagai berikut:

    2dfeb0aa ea47ad1c 8b042809 aa9387aa 700d0ea2

4.4 Analisis RSA

4.4.1 Analisis Pembangkitan Kunci

Berikut adalah contoh pembangkitan kunci pada RSA:

1. Bangkitkan 2 bilangan prima p dan q, misalnya p= 7 dan q =13
2. Cari n= p*q

   n= 7*13

   n=91
3. Cari $\phi(n)= (p-1) * (q-1)$

   $\phi(n) = (7-1) * (13-1)$

   $\phi(n) = 72$
4. Pilih e yang nilai nya relatif prima terhadap $\phi(n)$. Dalam hal ini penulis memilih 5 karena 5 relatif prima terhadap 72.
5. Tentukan kunci privat d dengan persamaan $d = (1 + a*\phi(n))/e$, dengan a adalah bilangan bulat yang dapat memenuhi. Sehingga untuk proses mencari nilai d sebagai berikut :

   a = 0 => d = 1/5 (tidak memenuhi)

   a = 0 => d = 73/5 (tidak memenuhi)

   a = 2 => d = 145/5 = 29 (memenuhi)

   Sehingga didapatkan kunci public (n = 91, e = 5) dan kunci privat (n = 91, d = 29)

4.4.2 Proses Enkripsi

Setelah e-dokumen telah diubah menjadi *message digest* maka proses selanjutnya adalah meenkripsi *message digest* menggunakan algoritma RSA dan kunci privat yang telah dibangkitan

Sebagai Contoh pesan yang akan dienkripsi adalah hasil *hash* pada contoh *hash* diatas yaitu “2DFEB0AAEA47AD1C 8B042809AA9387AA00D0EA2”.

1. Pertama, kita akan mengubah setiap karakter menjadi desimal melalui tabel ASCII

"50 68 70 69 66 48 65 65 69 65 52 55 65 68 49 67 56 66 48 52 50 56 48 57 65 65 57 51 56 55 65 65 48 48 68 48 69 65 50"

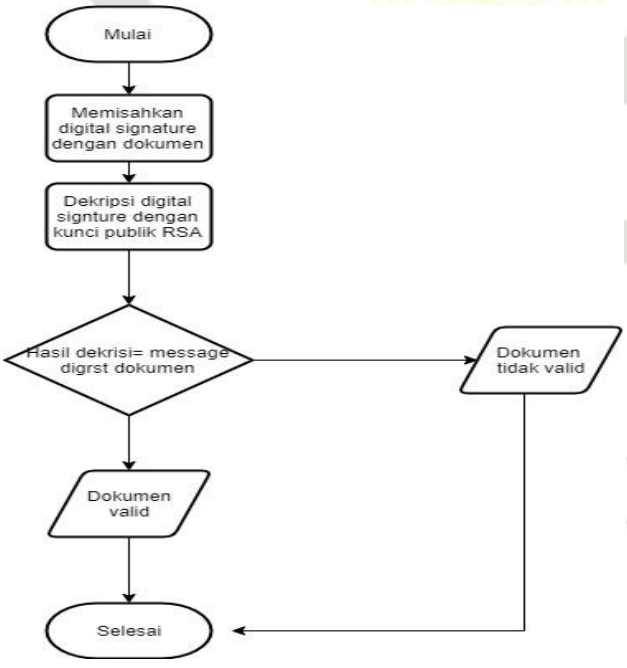
2. Selanjutnya ubah ke *chipertext* dengan rumus C= M^emod n

50^5 mod 91 = 85	52^5 mod 91 = 26	50^5 mod 91 = 85	65^5 mod 91 = 39
68^5 mod 91 = 87	55^5 mod 91 = 48	56^5 mod 91 = 49	65^5 mod 91 = 39
70^5 mod 91 = 70	65^5 mod 91 = 39	48^5 mod 91 = 55	48^5 mod 91 = 55
69^5 mod 91 = 62	68^5 mod 91 = 87	57^5 mod 91 = 57	69^5 mod 91 = 62
66^5 mod 91 = 40	49^5 mod 91 = 56	65^5 mod 91 = 39	69^5 mod 91 = 62
48^5 mod 91 = 55	67^5 mod 91 = 58	65^5 mod 91 = 39	50^5 mod 91 = 85
65^5 mod 91 = 39	56^5 mod 91 = 49	57^5 mod 91 = 57	
65^5 mod 91 = 39	66^5 mod 91 = 40	51^5 mod 91 = 25	
69^5 mod 91 = 62	48^5 mod 91 = 55	56^5 mod 91 = 49	
65^5 mod 91 = 39	52^5 mod 91 = 26	55^5 mod 91 = 48	

Sehingga diperoleh nilai *chipertext* nya yaitu:

"858770624055393962392648398756584940552685495557393957254948393955626285".

4.5 Proses Verifikasi Tandatangan



Gambar 4.3 Flowchart Proses Verifikasi Dokumen Surat Izin

Proses verifikasi dokumen untuk mebuktikan apakah dokumen sah atau tidak dimulai dengan merubah *digital signature* menjadi *hash* yang semula dengan melakukan deskripsi menggunakan kunci publik. Lalu, hasil dekripsi dibandingkan dengan *message digest* dokumen. Jika sama maka dokumen tersebut sah dan jika tidak sama dokumen tersebut tidak sah.

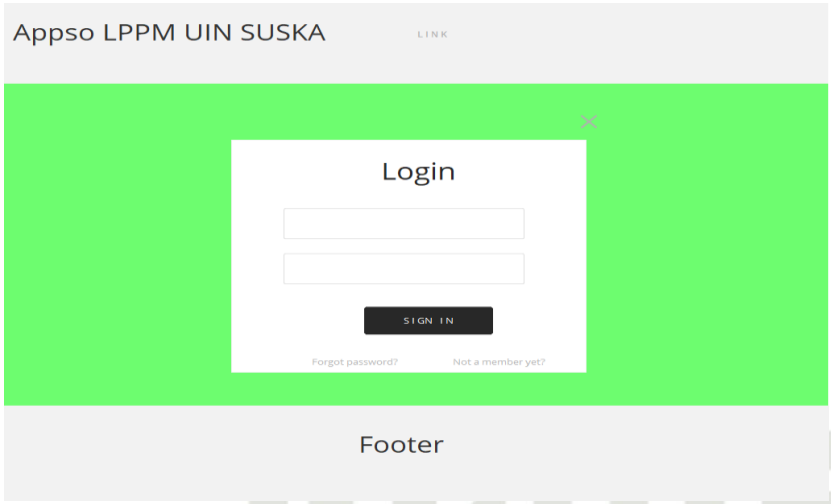
Berikut adalah contoh proses verifikasi pada e-dokumen:

1. Ubah *chipertext* e-dokumen menjadi pesan semula dengan persamaan
   M=C^dmod n
   C=858770624055393962392648398756584940552685495557393957254948393955626285
   d = 29
   85^{29}mod 91 = 50
   87^{29}mod 91 = 68 dan seterusnya
2. Sehinnga diperoleh nilai “50 68 70 69 66 48 65 65 69 65 52 55 65 68 49 67 56 66 48 52 50 56 48 57 65 65 57 51 56 55 65 65 48 48 68 48 69 65 50”
3. Ubah hasil yang telah diperoleh menjadi karakter. Sehingga menjadi seperti ini “2DFEB0AAEA47AD1C 8B042809AA9387AA00D0EA2”.
4. Bandingakan hasil deskripsi dengan *hash* e-dokumen. Karena hasil deskripsi sama dengan *hash* e-dokumen maka dokumen yang diverifikasi adalah dokumen yang sah.

4.6 Perancangan Antarmuka Aplikasi

4.6.1 Halaman login

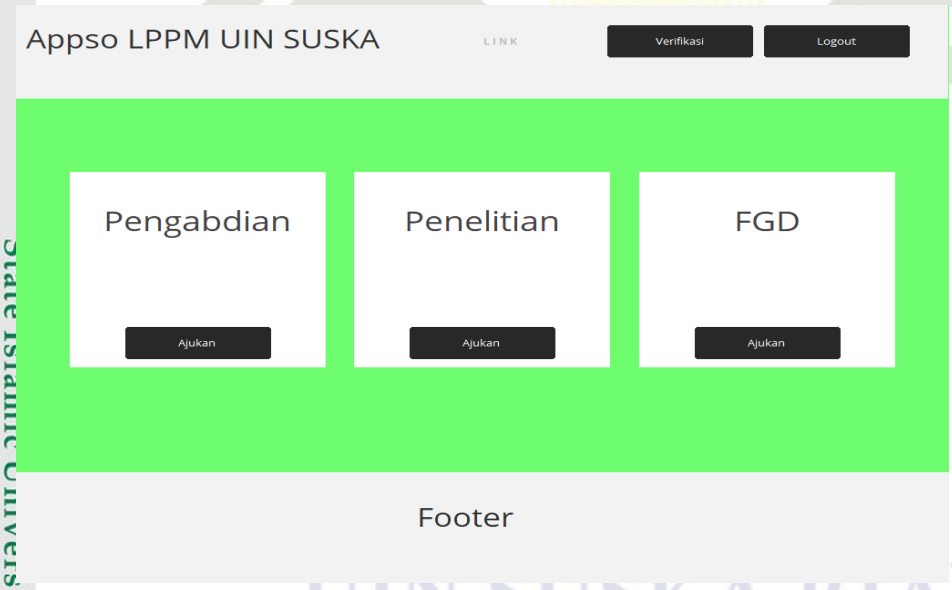
Pada halaman login terdapat 2 kolom dimana pengguna yaitu ketua LPPM maupun dosen harus mengisi NIK atau NIP dan juga password untuk dapat mengakses aplikasi *digital signature*.



Gambar 4.4 Halaman Login

4.6.2 Halaman Awal Dosen

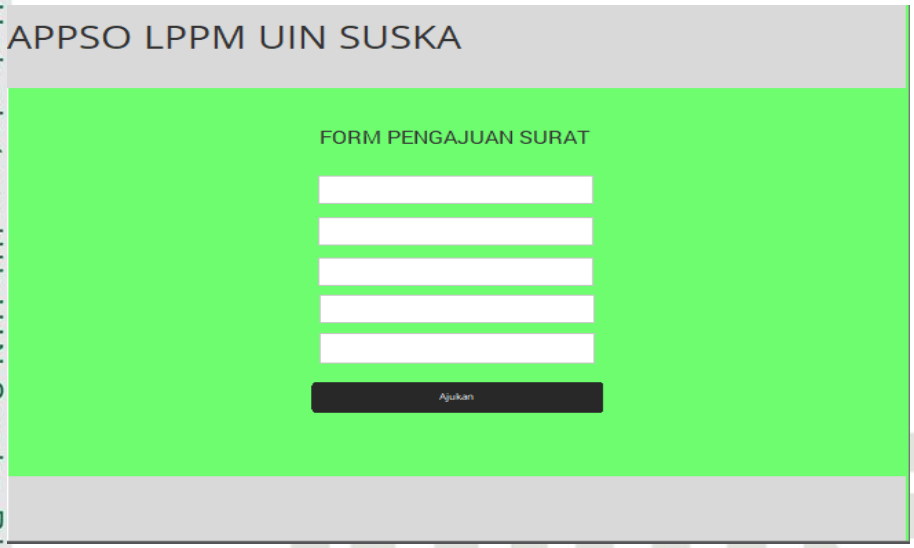
Pada dashboard dosen terdapat 3 pilihan surat yang ingin diajukan yaitu surat izin penelitian, izin pengabdian, dan izin fgd.



Gambar 4.5 Halaman Awal Dosen

4.6.3 Form Pengajuan Surat

Pengajuan surat harus dilakukan dengan mengisi form sesuai dengan jenis surat yang ingin diajukan pembuatannya. Berikut adalah gambar rancangan antarmuka form pengajuan surat.



Gambar 4.6 Form Pengajuan Surat

4.6.4 Halaman Verifikasi

Pada halaman verifikasi pengguna diharuskan mengunnggah dokumen surat yang ingin diverifikasi dan dokumen yang diunggah harus dengan format .pdf.

Gambar 4.7 Halaman Verifikasi Surat

4.6.5 Halaman Daftar Pengajuan Surat

Halaman ini adalah untuk ketua LPPM. Halaman ini menampilkan daftar pengajuan yang dilakukan dosen dan halaman ini digunakan untuk menandatangani dokumen surat yang diajukan.

Gambar 4.8 Daftar Pengajuan Surat

BAB VI
PENUTUP

6.1 Kesimpulan

Berdasarrkan tahap implementasi dan pengujian yang telah dilalui maka dapat diambil kesimpulan sebagai berikut:

1. Penerapan *digital signature* pada LPPM UIN SUSKA RIAU berhasil dilakukan
2. *Digital signature* yang diterapkan pada LPPM UIN SUSKA dapat memenuhi persyaratan umum tandatangan yaitu otentikasi, integritas, dan nirpeyangkalan.

6.2 Saran

Berikut adalah beberapa saran terkait penelitian selanjutnya yang dapat dilakukan berdasarkan Penelitian yang telah dilakukan, yaitu :

1. Membangun aplikasi berbasis android untuk penerapan *digital signature*
2. Menerapkan pada dokumen dengan format berbeda seperti dokumen *.doc*

DAFTAR PUSTAKA

Andi. (2003). *Memahami Model Enkripsi dan Security Data*. Yogyakarta: Wahana Komputer.

Ariyus, D. (2006). *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.

Ihwani, M. (2016). *Model Keamanan Informasi Berbasis Digital Signature dengan Algoritma RSA*.

KOMINFO. (2018). Penggunaan Tanda Tangan Digital di Indonesia Tumbuh Pesat.

Kromodimoeljo, S. (2010). *Teori Dan Aplikasi Kriptografi*. Jakarta.

Kurniawan, Y. (2004). *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung: Informatika Bandung.

Munir, R. (2006). *Kriptografi*. Bandung: Informatika Bandung.

Nugraha, A. (2016). *Penerapan Tanda Tangan Digital pada Sistem Pemerintahan Guna Mendukung E-Goverment*.

Refialy, L. (2015). *Pengamanan Sertifikat Tanah Digital Menggunakan Digital Signature SHA-512 dan RSA*.

Rionaldy, R. (2017). *Implementasi RSA sebagai Digital Signature pada Publikasi Arsip Elektronik Berbasis Web*.

Republik Indonesia. 1972. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Jakarta

DAFTAR RIWAYAT HIDUP

DATA PRIBADI		
	Nama	M. Hanafi
	Tempat / Tangal Lahir	Tiku, 09 April 1997
	Jenis Kelamin	Laki-Laki
	Status Pernikahan	Belum Menikah
	Anak Ke-	3 (Tiga)
	Tinggi Badan	165 cm
	Berat Badan	65 kg
	Kebangsaan	Indonesia
ALAMAT		
Alamat		Jl. Sukaramai, Bukit Kapur, Dumai.
Nomor HP		082169909899
Email		m.hanafi12@students.uin-suska.ac.id
RIWAYAT PENDIDIKAN		
Tahun 2003-2009		SDN 006 Bukit Kapur
Tahun 2009-2012		SMPN 5 Dumai
Tahun 2012-2015		SMKN 2 Dumai